REMARKS

In the first Office Action, the Examiner rejected claims 1-97 under the judicially created doctrine of obviousness-type double patenting based on a number of commonly owned pending applications and issued patents. The Examiner rejected claims 1-97 under 35 USC §102(b) as being anticipated by Ananda (US 5,495,411).

While Applicant does not agree with the double patenting rejection, due to the number of pending claims and the number of references alleged to render the claims unpatentable, Applicant submits herewith a terminal disclaimer to obviate the double patenting rejection.

Applicant respectfully disagrees with the Examiner's rejection under 35 USC §102(b) based on Ananda (US5,495,411) and traverses the rejection for the reasons described in detail below.

Reconsideration and re-examination of the application considering the following remarks is respectfully requested.

Information Disclosure Statements

The Examiner is respectfully requested to consider the documents and initial the Information Disclosure Statements filed on 9/21/06 relative to litigation of related U.S. patents. These Information Disclosure Statements were not included with the Office Action mailed to Applicant on 11/21/06.

Double Patenting

The Examiner rejected claims 1-97 for obviousness-type double patenting. While Applicant does not agree with the Examiner's position, Applicant submits herewith a Terminal Disclaimer to obviate the Examiner's rejection and advance the prosecution of this case.

Rejection Under 35 USC §102(b)

The Examiner rejected claims 1-97 as being anticipated by Ananda (US 5,495,411). Applicant respectfully disagrees and traverses the Examiner's rejection.

A rejection for anticipation requires that each and every element of Applicant's claims be disclosed explicitly or inherently in a single reference. As described in greater detail below, Applicant's claims include a number of features that are not disclosed in Ananda '411, and Applicant respectfully requests the Examiner to reconsider and withdraw the rejection.

<u>Summary of Ananda '411</u>

The '411 reference cited by the Examiner is directed to a software rental system using <u>continuous password verification</u>. The system allows a remote user computer system 150 to use application software downloaded from a central rental facility 180 <u>only while the remote user computer system 150 is electronically connected to the central rental facility</u>. This is accomplished by attaching additional header software 320 (Fig. 3) to the application software 310. Header software 320 includes a rental security manager 321 having modules for <u>authorization verification</u> 321A, <u>execution termination 321B</u>, encryption/decryption 321C, message processor 321D, password generation 321E, and password validation 321F.

During operation, a user provides a <u>user identification password</u> to access the central rental facility 122 (and remote computer 180), which compares the user password to <u>user identification information in registration database</u> 212 to determine if the user password is authorized (Col. 8, ll. 7-38). The user then selects an application program from the rental application database 214. In response, multiuser controller 222 transfers the selected application software 310 and header software 320 through modem 126 to the remote user computer system 150 (Col. 8, ll. 54-64). Central rental facility 122 records the <u>processor clock time</u> of the transfer and an application ID in a file for subsequent use in generating passwords, as well as sending an encrypted message with this information to the user computer system 150.

The rental security module 321 in the header software 320 on the user computer uses <u>1) the difference between the transfer time from the Central Rental Facility computer 180 and the local processor clock time, and 2) the user password entered to gain access to the Central Rental Facility, as input to a pseudorandom number generator to generate an authorization verification password</u> that is associated with the software by an application ID number. The user computer clock time, user ID password, and authorization verification password are sent to the Central Rental Facility, which also uses 1) the difference between the stored transfer time and the current clock time of the user computer, and 2) the user ID password as input to a pseudorandom number generator that generates an authorization verification password, which is sent back to the Rental Security Module on the user computer. The authorization verification passwords are compared by the Rental Security Module 321 to determine if the SW is authorized. <u>This process is repeated</u>

every 100 ms to ensure a continuous connection between the Central Rental Facility and the local user computer. If the authorization verification password comparison fails 3 times, execution of the application software program on the local user computer is terminated by termination module 321B (Col. 15, ll. 7-63).

Summary of Applicant's Claimed Invention

Applicant's invention as claimed in independent claims 1, 26, 55, and 87 is directed to a method for securing software to reduce unauthorized use that associates at least one identifier with the software to request authentication of the software by a resident authorized representative and to request exchange of information with a remote authorized representative. The identifier feature of the invention is best illustrated in Figs. 9, 62, 67, and 68 and described in Paras.[0165], [0291] and [0309] – [0314]. The identifier indicates that anti-piracy measures or copy protection and selective exchange of information is desired by the software distributor. The identifier may be in the form of a serial number, password, or other alphanumeric or binary string, for example and is preferably transparent to any systems that do not include an authorized representative or other module or device to implement copy protection so that the software may be used without restrictions on those systems or devices. The exchanged information may include repeated authorization and authentication, dynamic authorized representative process changes, updates/upgrades, patches, marketing or promotional purposes, quality assurance purposes, network monitoring and metering, error and usage information, etc. As also described and illustrated in Figs. 67-68, the identifier may be included in a unique file prefix, file suffix, file extension, embedded within the content, or as a binary code, for example.

As illustrated and described with reference to Fig. 68, software that includes at least one identifier to request authentication by a resident authorized administrator and to request exchange of information with a remote authorized administrator is associated with the software prior to being distributed to the user. The identifier is detected by an authorized representative entity installed on or in the user device and selectively exchanges information with a remotely located authorized representative. The user device resident authorized representative entity then determines whether attempted access to the software is authorized based on registration information and/or an authentication code associated with the software. The registration

information and authentication code(s) may be associated with a particular user device or a group of authorized devices.

<u>Distinguishing Features of Applicant's Claimed Invention</u>

Applicant's claimed invention includes a number of features that are not disclosed in Ananda. At least one feature or limitation in each of the following claims is not disclosed in Ananda. However, the following is not intended to be an exhaustive description and various other features and/or claims may include other distinguishing limitations that are not disclosed in Ananda and not explicitly described below.

In general, Ananda '411 does not disclose software with an identifier that triggers an authentication and selective exchange of information as disclosed and claimed. The Examiner cites various passages from Ananda that relate to the central rental facility and the header software with its incorporated rental security manager 321 that generates authorization verification passwords. However, it is not clear from the rejection how these features are being applied to various elements of Applicant's claims. It appears from the rejection of various claims that the Examiner's interpretation is necessarily inconsistent in rejecting an independent claim and its corresponding dependent claims. For example, it appears the Examiner is interpreting the header module as the identifier associated with the software, but also as the authorized representative entity that detects the identifier associated with the software in rejecting claim 1. This interpretation appears to change in the rejection of dependent claims where the cited passages refer to the authorization verification password generated by the rental security manager, such that the Examiner is indicating that the authorization verification password is now the element that anticipates Applicant's claimed "identifier". Since each dependent claim incorporates all of the limitations of the claims from which it depends, the Examiner must consistently interpret a particular feature disclosed by Ananda throughout the related independent and dependent claims.

The Examiner is respectfully requested to clarify the elements of Ananda that anticipate each element of Applicant's claims rather that reciting the entire claim followed by a citation to multiple columns/lines in Ananda that purportedly anticipate all the elements of the claim to facilitate Applicant's understanding and analysis of the Examiner's position to provide relevant arguments and/or claim amendments as necessary. For example, Ananda discloses a user password that is associated with

a registration database of user information, a header module that includes a rental security manager having modules to generate authorization verification passwords, perform encryption/decryption, terminate application execution, etc. The Examiner is respectfully requested to identify which of these elements is purported to anticipate Applicant's claimed identifier or plurality of identifiers, and which element anticipates the authorized representative entity that detects the identifier, and which element anticipates the remote authorized representative entity. Similarly, the Examiner is requested to identify which feature of Ananda anticipates Applicant's registration information associated with a user device, and how/where Ananda discloses registration information associated with a particular device or group of devices as disclosed and claimed by Applicant.

With respect to claim 1, Ananda does not disclose associating at least one identifier with the software prior to distribution of the software that is detectable by a resident authorized representative to request authentication of the software and to request selective exchange of information with a remote authorized representative. If the Examiner is interpreting the header module disclosed by Ananda as anticipating the "identifier" claimed by Applicant, the header module is not "detected" by the user computer, and can not function as or anticipate both the claimed "identifier" and the "authorized representative". Prior to transferring the application program from the central rental facility to the user computer, there is no authorized representative entity on the user computer that can detect anything. Alternatively, if the Examiner is interpreting the authorization verification password or user password disclosed by Ananda as the "identifier" claimed by Applicant, then neither of those is associated with the software prior to distribution and distributed with the software as required by claim 1. Furthermore, neither password is detectable to request authentication of the software by a resident authorized representative, or to request selective exchange of information with a remote authorized representative as claimed.

As per claims 2 and 3, Ananda does not disclose selective exchange of information that includes updates, upgrades, patches, marketing information, promotional information, etc. The passage relied upon by the Examiner relates to updating and monitoring functions of the central rental facility and not to the exchange of information with the user computer.

As per claim 4, there is no disclosure of dynamically updating the authorized representative as claimed.

As per claim 5, Ananda transfers the application software and header module to the user computer at the beginning of session, presumably with the alleged "identifier" that is detected to request exchange of information. The instructions to repeat authentication disclosed by Ananda are transferred with the application program and not in response to detecting an "identifier" as claimed.

As per claim 9, it is unclear what the Examiner alleges anticipates Applicant's claimed "identifier". However, Ananda does not disclose any feature that is embedded within a file of the software component.

As per claim 11, Ananda discloses encrypting the authorization verification message but does not disclose any "identifier" or encrypting the identifier. The authorization verification message can not function as such an identifier because it is not associated with the software prior to distribution and is not distributed with the software. Similarly, the header module and/or rental security manager is associated prior to distribution, but is not encrypted. As such, neither meets Applicant's claim limitations.

As per claim 13, Ananda discloses only distribution of the software via a telephone network and not via a computer readable storage medium as claimed.

As per claim 14, Ananda does not disclose any detection of an identifier to trigger authentication or exchange of information as disclosed and claimed by Applicant. The header module executes without regard to any identifier and therefore does not perform the authorization process based on detection of the at least one identifier as claimed. Prior to transfer of the application program and header module to the user computer, there is nothing than can detect the purported "identifier" installed on the user computer.

As per claim 15, Ananda does not disclose registration information associated with the software. The only registration information disclosed by Ananda is contained in the registration database at the central rental facility and includes a user identification password, which is not associated with the software.

As per claim 16, the registration information disclosed by Ananda is not associated with a user device as claimed. Rather, the registration information is associated with the user upon initial access to the central rental facility via the user identification password.

As per claims 22-23, none of the registration information, header module, or authorization verification passwords disclosed by Ananda are included in a filename

for a software component, and none are included as a filename prefix, suffix, or extension as claimed.

As per claim 26, Ananda does not disclose a plurality of identifiers associated with the software prior to distribution including at least one that is detectable by a resident authorized representative to request authentication of the software and to request selective exchange of information with a remote authorized representative. In addition, Ananda requires continuous contact with the central rental facility, a remote authorized representative entity. Ananda does not disclose an identifier that is detectable by a resident authorized representative entity as claimed. If the Examiner interprets the authorization verification password as the "identifier", it is not associated with the software prior to distribution. If the Examiner interprets the header module or any of its sub-modules as the "identifier" then there is nothing on the user computer to "detect" the identifier.

As per claim 27, none of the features disclosed by Ananda, including the authorization verification passwords, the header module, and the rental security manager are entered prior to transferring the software. If the Examiner interprets the user identification password entered to access the central rental facility as anticipating the "authentication code" that is one of the plurality of "identifiers" then it is not associated with the software prior to distribution, and is not detected to trigger authorization as claimed by Applicant.

As per claim 28, Ananda does not disclose any identifier that requests selective exchange of information and that triggers instructions for the resident authorized administrator to contact a remote authorized representative at predetermined intervals. While the header module attempts to contact the central rental facility at predetermined intervals, there is no disclosure of an identifier that is required to trigger operation of the header module as disclosed and claimed by Applicant.

As per claim 29, the only information exchanged by the user computer and central rental facility during execution of the application program is the information needed by the pseudorandom number generator to generate the authorization verification passwords, i.e. the transfer time, the user computer processor clock time, and the user identification password. There is no disclosure of exchanging information selected from the group consisting of updates, upgrades, patches, marketing information, etc. as claimed.

Similarly, as per claim 30, Ananda does not disclose any method for dynamic authorized representative changes after detecting a request for selective exchange of information as claimed by Applicant. Rather, Ananda suggests that the header module and application program must be transferred for each execution of the application program because the transfer time is required for the authorization verification passwords.

Limitations of claim 31-39 have been previously addressed.

As per claim 40, Ananda does not disclose any detection step. The header module executes without regard to the presence or absence of any identifier. As such, Ananda does not anticipate performing a process to determine whether an attempted access to the software is authorized based on detection of the at least one identifier.

As per claims 41-42, Ananda does not disclose registration information associated with the software or with a user device, but instead discloses that the registration information is associated with the user as previously addressed.

As per claim 43, Ananda does not generate at least one authentication code based on the registration information and associate the authentication code with the software as claimed. The authorization verification passwords disclosed by Ananda are independently generated by the user computer and the central rental facility. The messages exchanged include the user computer clock time and the transfer time of the software from the initial transfer to the user computer. Because the transfer time is required to determine the authorization verification password, Ananda does not associate the authentication code with the software as claimed by Applicant.

As per claims 48-49, as described above any of the features of Ananda that could be interpreted as an "identifier" are not included in any part of the file name for at least one component of the software as claimed by Applicant.

As per claim 52, Ananda does not disclose associating at least one identifier with the software to request selective exchange of information and then selectively exchanging information with a remote authorized representative. Again, if the header module is alleged to anticipate the "identifier", then Ananda does not disclose any other feature that could function as the authorized representative installed on the user device. Furthermore, the only information exchanged is the information related to generation of the authorization verification passwords.

As per claim 53, Ananda does not disclose a resident authorized representative and therefore does not disclose exchanging information with a resident authorized representative. In contrast, Ananda requires continuous communication with a remote authorized representative.

As per claim 55, Ananda does not disclose at least one resident authorized representative entity installed on or in a user device in addition to at least one identifier associated with the software to designate the software for protection from unauthorized use and at least one identifier associated with the software to request selective communication with a remote authorized representative. In addition, Ananda does not disclose any step related to detecting an identifier. The header module and embedded rental security manager executes without regard to whether any type of "identifier" is "detected". Ananda does not disclose controlling access to the software in addition to selectively exchanging information with the remote authorized representative.

As per claim 56, Ananda does not disclose a resident authorized representative and therefore does not disclose instructions for the resident authorized representative to contact a remote authorized representative as claimed.

As per claims 57-58, the only information exchange disclosed by Ananda is the authorization verification message that includes the information for the pseudorandom number generator to generate the authorization verification passwords. There is no disclosure of exchanging any of the kinds of information claimed by Applicant. Ananda discloses updating and management of the central rental facility, not an authorized representative entity installed on the user computer/device as claimed by Applicant.

The limitations of claims 59-77 have been addressed above and are incorporated here by reference.

As per claims 78-80, Ananda does not disclose controlling access by preventing transfer of the software to a second user device. The only measure disclosed by Ananda to prevent unauthorized use of the software is to require continuous communication with the central rental facility. Ananda acknowledges that the software may be transferred to another computer, but will not work because any subsequent authorization verification passwords will include the proper transfer time from the central rental facility (because this information is deleted from the central rental facility when the connection is lost). As such, Ananda does not anticipate these claims.

As per claim 82, Ananda does not disclose providing limited access to the software. The only action disclosed by Ananda is termination of the application program if the user is not authorized or if communication with the central rental facility is lost.

As per claim 87, Ananda does not disclose any detecting steps as described previously. As such, Ananda does not disclose detecting at least one identifier associated with the software indicating that protection from unauthorized use is desired or detecting at least one identifier associated with the software to request selective exchange of information.

As per claim 88, none of the features disclosed by Ananda is related to the filename of the software.

As per claim 92, Ananda does not disclose authorization information associate with the user device.

As per claim 93, Ananda does not generate an authentication code based on registration information associated with the user device and does not compare the authentication code with a previously generated authentication code to determine if the user device is authorized.

As per claim 94, Ananda does not determine if at least a portion of system information associated with the user device matches system information encoded within the authentication code associated with the software.

As per claim 95, Ananda does not disclose registration information that includes hardware-specific information. The registration information disclosed by Ananda is related to the user and stored in the central rental facility registration database, which is accessed via the user identification password.

As per claim 96, the representative entity of Ananda is located at the central rental facility. Ananda does not disclose an authorized representative entity installed on or in the user device.

Summary

Applicant's method for securing software using an identifier to indicate that protection from unauthorized use is desired and an identifier to indicate that exchange of information is desired as disclosed and claimed in independent claims 1, 26, 55, and 87 includes a number of features that are not disclosed in, and therefore not anticipated by Ananda (US 5,495,411). In addition, numerous features found in dependent claims are not disclosed by Ananda '411. Applicants have made a genuine effort to respond to the Examiner's rejections and advance prosecution of this application. Applicants believe that all substantive and formal requirements for patentability have been met and that this case is in condition for allowance, which action is respectfully requested.

No additional fee other than the extension of time fee of $510 and the terminal disclaimer fee of $65 is believed to be due as a result of the filing of this paper. However, please charge any required fees or apply credits to **Deposit Account 50-2841**.

Respectfully submitted:

David S. Bir
Registration No. 38,383

May 21, 2007

Bir Law, PLC
13092 Glasgow Ct.
Plymouth, MI 48170-5241
(734) 927-4531